Zabezpečení uživatelských účtů zaměstnanců multifaktorovou autentizací

Článek 1

Úvodní ustanovení

1) Rektor Univerzity Hradec Králové (dále jen *„univerzita“*) vydává tento rektorský výnos za účelem zvýšení zabezpečení informačních systémů univerzity z následujících důvodů:

   a) Univerzita je ve svěřené působnosti v oblasti veřejné správy orgánem veřejné moci, na který se vztahují ustanovení zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a jeho prováděcích předpisů.

   b) Národní úřad pro kybernetickou a informační bezpečnost (dále jen *„NÚKIB“*) v rámci preventivních kroků vydal v souvislosti s kritickou hrozbou kyberšpionáže a dalších kybernetických útoků varování, v němž nabádá organizace řídíc se zákonem o kybernetické bezpečnosti, k ostražitosti proti nejčastěji používaným technikám útoků a k provedení aktualizace informačních systémů a jejich komponent tak, aby nedocházelo ke zneužití známých zranitelností.

   c) V hodnocení kybernetických incidentů, které NÚKIB zveřejňuje na svých webových stránkách, je zmíněn rostoucí trend hrozeb v oblasti tzv. *phishingu*, *spear-phishingu* a sociálního inženýrství s následnou kompromitací uživatelských účtů. Hrozby zaznamenávají pravidelně i automatizované systémy kontrol příchozí poštovní komunikace v rámci univerzitní infrastruktury. Zavedení vícefaktorové autentizace snižuje rizika zneužití účtů a poštovních schránek uživatelů.

   d) V návaznosti na doporučení Výboru kybernetické bezpečnosti byl ze strany vedení univerzity pověřen vedoucí Oddělení informačních systémů (dále jen OIT) koordinací zvýšení zabezpečení informačních systémů univerzity postupným nasazením vícefaktorové autentizace (dále jen *„MFA“*) pro bezpečné přihlašování.

Článek 2

Harmonogram nasazení MFA

1) Rektor tímto opatřením ukládá součástem univerzity, aby:

   a) do 60 dnů od nabytí účinnosti tohoto opatření u jednotlivých zaměstnanců stanovili způsob zabezpečení ve smyslu čl. 3 odst. 1 tohoto opatření a informaci předali dle informací na adrese:

      uhk.cz/m365-mfa-form,

   b) nejpozději do 1. 5. 2025 zajistili, že zaměstnanci budou mít způsob zabezpečení stanovený dle písm. a) tohoto odstavce zaregistrovaný v portálu Microsoft 365 dle návodů, které jsou k dispozici na adrese:

      uhk.cz/m365-mfa.

   c) V případě, kdy není metoda vícefaktorové autentizace u konkrétního zaměstnance vyžadována z objektivních důvodů (osoba, která nemá zřízen účet do počítačové sítě, přístupy do poštovní schránky, přístupy k ostatním informačním systémům univerzity, případně se jedná o osobu se závažným zdravotním handicapem), je třeba tuto informaci předat vedoucímu OIT. Oprávněné žádosti o výjimku budou posuzovány v rámci Výboru kybernetické bezpečnosti, který si může vyžádat doplňující informace.

2) Rektor ukládá kvestorovi a prorektorovi pro strategii, rozvoj a digitalizaci, aby vedoucí OMO nejpozději do 1. 3. 2025 ve spolupráci s vedoucím OIT navrhla a zrealizovala změny v dokumentech a postupech souvisejících se vznikem a skončením pracovněprávních vztahů, které zahrnou nastavení metody MFA a správy poskytnutých bezpečnostních tokenů do standardních procesů univerzity.

3) Rektor dále ukládá vedoucímu OIT na základě dat získaných dle odst. 1 tohoto článku stanovit potřeby hardwarového vybavení a připravit harmonogram nasazování MFA na jednotlivých fakultách, celouniverzitních a rektorátních odděleních (dále jen *„harmonogram“*). Na základě harmonogramu ukládá OIT podniknout nezbytné kroky k jeho realizaci.

4) Veškeré postupy a podrobnosti související s tímto výnosem budou dostupné na webových stránkách univerzity na adrese:

   uhk.cz/m365-mfa

Článek 3

Způsob realizace MFA

1) Vícefaktorová autentizace bude na univerzitě realizována některou z uvedených metod:

   a) využitím ověřovací aplikace nainstalované na chytrém mobilním telefonu nebo

   b) využitím fyzického zařízení pro elektronické ověření identity uživatele (tzv. bezpečnostního tokenu),

   c) zasíláním potvrzovacích SMS kódů (doporučeno pouze jako záložní metoda).

2) Zaměstnanci si mohou zaregistrovat metody vícefaktorové autentizace podle odst. 1 písm. a) nebo b) dle detailního návodu na adrese:

   uhk.cz/m365-mfa-navod.

3) Zaměstnancům je umožněno využívat vícefaktorovou autentizaci prostřednictvím služebního i soukromého telefonu podle odst. 1 písm. a) nebo c) tohoto článku nebo bezpečnostního tokenu podle odst. 1 písm. b) tohoto článku.

4) Technické požadavky a podporu metody MFA poskytuje zaměstnancům OIT. Zaměstnanci se mohou obrátit na pracovníky koncové podpory uživatelů prostřednictvím webové aplikace helpdesku (helpdesk-cit.uhk.cz), e-mailu (helpdesk-oit@uhk.cz), případně osobně.

5) Standardní proces pořizování a správu bezpečnostních tokenů ve vlastnictví univerzity podle odst. 1 písm. b) tohoto článku zajišťuje OIT. Žádost o poskytnutí bezpečnostního tokenu podá příslušný vedoucí zaměstnanec prostřednictvím závazné objednávky zaevidované v EIS Magion. Informace o doporučených tokenech a kontakt na prodejce je na adrese:

   uhk.cz/m365-mfa.

6) Náklady spojené s pořízením bezpečnostního tokenu, případně služebního telefonu se hradí z prostředků pracoviště, na kterém je příslušný zaměstnanec zaměstnán.

Článek 4

Závěrečná ustanovení

Toto opatření nabývá platnosti dnem podpisu rektora a účinnosti od 1. 3. 2025.

V Hradci Králové dne 04. 03. 2025

doc. RNDr. Jan Kříž, Ph.D., v. r.
rektor